

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005 年 8 月 11 日 (11.08.2005)

PCT

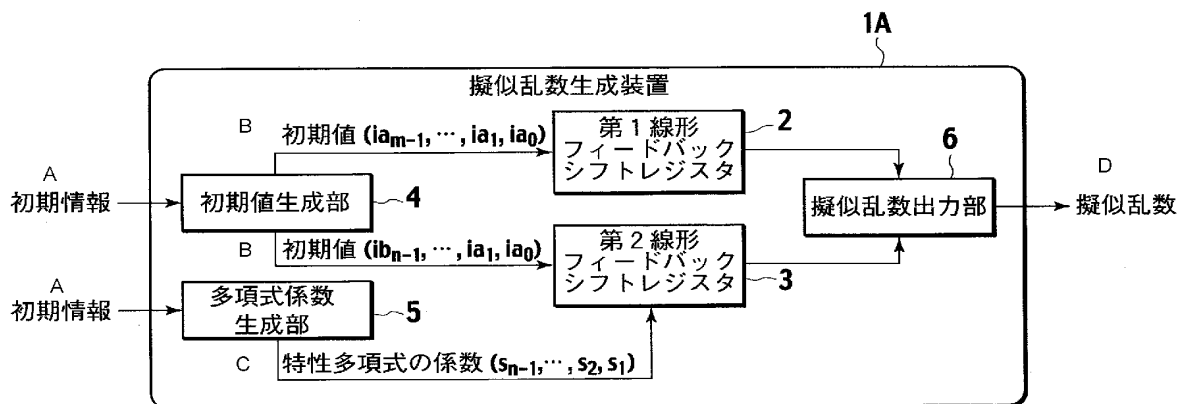
(10) 国際公開番号
WO 2005/073842 A1

- (51) 国際特許分類⁷: G06F 7/58, H03K 3/84 (74) 代理人: 三好 秀和 (MIYOSHI, Hidekazu); 〒1050001 東京都港区虎ノ門 1 丁目 2 番 8 号 虎ノ門平塔ワー Tokyo (JP).
- (21) 国際出願番号: PCT/JP2005/001211
- (22) 国際出願日: 2005 年 1 月 28 日 (28.01.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2004-023335 2004 年 1 月 30 日 (30.01.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 日本ビクター株式会社 (VICTOR COMPANY OF JAPAN, LIMITED) [JP/JP]; 〒2218528 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 Kanagawa (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてののみ): 猪羽 渉 (INOHA, Wataru). 日暮 誠司 (HIGURASHI, Seiji).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,

[続葉有]

(54) Title: PSEUDO RANDOM NUMBER GENERATION DEVICE AND PSEUDO RANDOM NUMBER GENERATION PROGRAM

(54) 発明の名称: 擬似乱数生成装置および擬似乱数生成プログラム



A... INITIAL INFORMATION

1A... PSEUDO RANDOM NUMBER GENERATION DEVICE

B... INITIAL VALUE

4... INITIAL VALUE GENERATION UNIT

5... POLYNOMIAL COEFFICIENT GENERATION UNIT

C... CHARACTERISTIC POLYNOMIAL COEFFICIENT

2... FIRST LINEAR FEEDBACK SHIFT REGISTER

3... SECOND LINEAR FEEDBACK SHIFT REGISTER

6... PSEUDO RANDOM NUMBER OUTPUT UNIT

D... PSEUDO RANDOM NUMBER

(57) Abstract: A pseudo random number generation device (1) includes a first linear feedback shift register (2), a second linear feedback shift register (3), an initial value generation unit (4), a polynomial coefficient generation unit (5), and a pseudo random number output unit (6). The initial value generation unit (4) generates an initial value and supplies it to the first linear feedback shift register (2) and the second linear feedback shift register (3). The polynomial coefficient generation unit (5) generates a characteristic polynomial coefficient and supplies it to the second feedback shift register (3). The pseudo random number output unit (6) generates a pseudo random number from the exclusive OR of each bit according to the bit string successively output from the first linear feedback shift register (2) and the second linear feedback shift register (3) and outputs it.

[続葉有]



WO 2005/073842 A1



IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約: 擬似乱数生成装置(1)は、第1線形フィードバックシフトレジスタ(2)、第2線形フィードバックシフトレジスタ(3)、初期値生成部(4)、多項式係数生成部(5)および擬似乱数出力部(6)を有する。初期値生成部(4)は、初期値を生成し、第1線形フィードバックシフトレジスタ(2)および第2線形フィードバックシフトレジスタ(3)へ供給する。多項式係数生成部(5)は、特性多項式の係数を生成して第2線形フィードバックシフトレジスタ(3)へ供給する。擬似乱数出力部(6)は、第1線形フィードバックシフトレジスタ(2)および第2線形フィードバックシフトレジスタ(3)から順次出力されるビット列を基に、各ビットの排他的論理和から擬似乱数列を生成、出力する。

明 細 書

擬似乱数生成装置および擬似乱数生成プログラム

技術分野

[0001] 本発明は、暗号通信に利用される擬似乱数を生成する擬似乱数生成装置および擬似乱数生成プログラムに関する。

背景技術

[0002] 現在、電話や無線、インターネット等におけるデータ通信では、通信されるデータを第三者による盗聴や改ざんから保護するために、データの暗号化が行われている。データの送信側では、暗号鍵を用いて送信するデータを暗号化した後送信し、受信側では、その暗号化されたデータを受信すると、復号鍵を用いて復号化しデータを得ている。もしこの時、第三者がデータを傍受しても、正当な復号鍵を持たないため暗号化されたデータを復号することができず、また、意図したデータの改ざんを行うこともできない。

[0003] このような暗号化の方式には、共通鍵暗号方式や公開鍵暗号方式があり、それぞれの特徴をいかして利用される条件に応じて選択される。いずれの方式であっても、暗号鍵によって通信されるデータの安全性が保障されており、その暗号鍵は容易に推測されないように擬似乱数を用いる方法が知られている。

[0004] 例えば、線形フィードバックシフトレジスタによる擬似乱数の生成方法では、乱数生成のための比較的短い初期値からデータ長の長い擬似乱数列を生成することができるため、複数の装置で同じ擬似乱数を生成しようとするとき、初期値を共有するだけで良い。また、一般に、特定の条件を満たす原始多項式を特性多項式とする複数の線形フィードバックシフトレジスタを組み合わせることで、生成される擬似乱数の予測が困難な擬似乱数生成装置を実現可能なことが知られている。さらに、初期値を共有しなくても、複数の線形フィードバックシフトレジスタの選択情報を共有化することで、同じ擬似乱数列を生成することも可能である（例えば、特開平10-91066号公報参照）。

[0005] しかしながら、線形フィードバックシフトレジスタを用いた擬似乱数生成装置では、

たとえ非線形な処理を組み合わせた方法であっても、ある特定のアルゴリズムで擬似乱数が生成されるため、初期値や生成される擬似乱数列の一部からその後生成される擬似乱数が推測される恐れがあった。

- [0006] また、複数の線形フィードバックシフトレジスタからいくつかのレジスタを選択して擬似乱数を生成する場合には、生成される擬似乱数列の推測は困難になるものの、任意の係数を特性多項式とする線形フィードバックシフトレジスタを組み合わせると、生成される擬似乱数列が必ずしもM系列(Maximum length sequences)とはならず、短い周期で同じ擬似乱数列を繰り返し生成してしまうという問題があるため、予め特定の条件を満たす多項式を多数用意した中から選択して組み合わせる必要があった。これは実際の処理では、常に利用するわけではない線形フィードバックシフトレジスタを実装する必要があり効率的ではなかった。

発明の開示

- [0007] 本発明は、生成される擬似乱数列や送受信されるデータを観測されても、その後生成される擬似乱数列の推測が困難な暗号通信に好適な擬似乱数生成装置および擬似乱数生成プログラムを提供することを目的とする。
- [0008] 上記目的を達成するために、第1の態様に係る発明は、所定のビット長の擬似乱数列を生成する擬似乱数生成装置であって、m段のシフトレジスタを有し、所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタと、n段のシフトレジスタを有し、所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタと、所定の条件に従って、前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタへ供給する初期値生成部と、所定の条件に従って、前記第2の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第2の線形フィードバックシフトレジスタへ供給する多項式係数生成部と、前記第1の線形フィードバックシフトレジスタの特性多項式として原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶部と、所定の条件に従って、前記原始多項式記憶部に記憶されている原始多項式を1つ選択し、その原始

多項式の係数を特性多項式の係数として前記第1の線形フィードバックシフトレジスタへ供給する原始多項式選択部と、前記第1の線形フィードバックシフトレジスタから出力されるビット列と、前記第2の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力部と、を備える擬似乱数生成装置を要旨とする。

[0009] また、第2の態様に係る発明は、第1の態様に係る発明において、前記擬似乱数生成装置は、前記原始多項式選択部によって選択された前記原始多項式の識別情報、前記初期値生成部によって生成された前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成部によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成し、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第1のフィードバックシフトレジスタと前記第2のフィードバックシフトレジスタとの各初期値を抽出して前記第1の線形フィードバックシフトレジスタと前記第2の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第2の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択部に供給する通信部を備え、前記原始多項式選択部は、前記通信部によって抽出された前記識別情報を基に、前記原始多項式記憶部に記憶されている原始多項式を1つ選択し、その原始多項式の係数を前記第1の線形フィードバックシフトレジスタへ供給することを要旨とする。

[0010] また、上記目的を達成するために、第3の態様に係る発明は、所定のビット長の擬似乱数列を生成するコンピュータによって実行される擬似乱数生成プログラムであって、当該擬似乱数生成プログラムは、前記コンピュータを、m段のシフトレジスタを有し、所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタと、n段のシフトレジスタを有し、所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタと、所定の条件に従って、前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの

初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタへ供給する初期値生成手段と、所定の条件に従って、前記第2の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第2の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、前記第1の線形フィードバックシフトレジスタの特性多項式として原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶手段と、所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を特性多項式の係数として前記第1の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、前記第1の線形フィードバックシフトレジスタから出力されるビット列と、前記第2の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段として機能させる擬似乱数生成プログラムを要旨とする。

[0011] また、第4の態様に係る発明は、第3の態様に係る発明において、前記擬似乱数生成プログラムは、前記コンピュータを、前記原始多項式選択手段によって選択された前記原始多項式の識別情報、前記初期値生成手段によって生成された前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成し、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第1のフィードバックシフトレジスタと前記第2のフィードバックシフトレジスタとの各初期値を抽出して前記第1の線形フィードバックシフトレジスタと前記第2の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第2の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、前記原始多項式選択手段は、前記通信手段によって抽出された前記識別情報を基に、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択

し、その原始多項式の係数を前記第1の線形フィードバックシフトレジスタへ供給することを要旨とする。

図面の簡単な説明

- [0012] 図1は、第1の実施形態における擬似乱数生成装置の機能構成を示す図である。
- 図2は、第1線形フィードバックシフトレジスタの回路構成を示す図である。
- 図3は、第2線形フィードバックシフトレジスタの回路構成を示す図である。
- 図4は、第1の実施形態における擬似乱数生成の処理を示すフローチャートである。
- 図5は、第1線形フィードバックシフトレジスタと第2線形フィードバックシフトレジスタの値の遷移を示す図である。
- 図6は、第2の実施形態における擬似乱数生成装置の機能構成を示す図である。
- 図7は、第2の実施形態における擬似乱数生成の処理を示すフローチャートである。
- 図8は、第3の実施形態における擬似乱数生成装置の機能構成を示す図である。
- 図9は、第3の実施形態における擬似乱数生成の処理を示すフローチャートである。

発明を実施するための最良の形態

- [0013] 本発明の実施形態を、図1～図9を用いて説明する。なお、擬似乱数生成装置1が生成する擬似乱数のビット長を $h+1$ とする。

[0014] <第1の実施形態>

第1の実施形態における擬似乱数生成装置1Aは、図1に示すように、第1線形フィードバックシフトレジスタ2、第2線形フィードバックシフトレジスタ3、初期値生成部4、多項式係数生成部5、および擬似乱数出力部6を有する。

- [0015] 第1線形フィードバックシフトレジスタ2は、 m 次の線形フィードバックシフトレジスタであり、 m 個のフリップフロップ回路を有する(詳細については後述)。また、第2線形

フィードバックシフトレジスタ3は、 n 次の線形フィードバックシフトレジスタであり、 n 個のフリップフロップ回路を有する(詳細については後述)。

[0016] 初期値生成部4は、外部から入力される初期情報、あるいは予め定められた所定の条件、例えば、日時情報のように常に変化する情報や熱雑音等の物理現象を利用して得られる条件に従って、第1線形フィードバックシフトレジスタ2を構成する各フリップフロップの初期値 ia ($ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0$)を生成し、第1線形フィードバックシフトレジスタ2へ供給する機能と、第2線形フィードバックシフトレジスタ3を構成する各フリップフロップの初期値 ib ($ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0$)を生成し、第2線形フィードバックシフトレジスタ3へ供給する機能を有する。ただし、第1線形フィードバックシフトレジスタ2からの出力が常に“0”にならないよう、少なくとも初期値 ia_{m-1} 乃至 ia_0 のいずれか1つが値“1”であり、同様に、少なくとも初期値 ib_{n-1} 乃至 ib_0 のいずれか1つが値“1”であることとする。

[0017] また、多項式係数生成部5は、外部から入力される初期情報、あるいは予め定められた所定の条件、例えば、日時情報のように常に変化する情報や熱雑音等の物理現象を利用して得られる条件に従って、第2線形フィードバックシフトレジスタ3の特性多項式の係数 s ($s_{n-1}, s_{n-2}, \dots, s_2, s_1$)を生成し、第2線形フィードバックシフトレジスタ3へ供給する機能を有する。

[0018] また、擬似乱数出力部6は、第1線形フィードバックシフトレジスタ2から順次出力されるビット列 ra ($ra_0, ra_1, \dots, ra_{h-1}, ra_h$)と、および第2線形フィードバックシフトレジスタ3から順次出力されるビット列 rb ($rb_0, rb_1, \dots, rb_{h-1}, rb_h$)とに基づいて、各ビットの排他的論理和を求め所定のビット長の擬似乱数 r ($r_0, r_1, \dots, r_{h-1}, r_h$)を生成し、出力する機能を有する。

[0019] 第1線形フィードバックシフトレジスタ2は、図2に示すように、 m 個のフリップフロップ回路とAND回路、およびXOR回路から構成される。この第1線形フィードバックシフトレジスタ2の特性多項式は、予め定められた原始多項式 $a_m x^m + a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \dots + a_2 x^2 + a_1 x + a_0$ (ただし、 $a_m = 1$ 及び $a_0 = 1$)であり、AND回路それぞれに原始多項式の係数 a (a_{m-1}, \dots, a_1)が設定される。

[0020] 従って、 $a_i = 0$ ($0 < i < m$)の時は、フリップフロップ FA_{i-1} ($0 < i < m$)から出力される値に関係

なくAND回路からは“0”が出力され、 $a_i=1$ ($0 < i < m$) の時は、フリップフロップ FA_{i-1} ($0 < i < m$) から出力される値が出力される。

[0021] 第2線形フィードバックシフトレジスタ3は、図3に示すように、 n 個のフリップフロップ回路とAND回路、およびXOR回路から構成される。この第2線形フィードバックシフトレジスタ3の特性多項式を $b_n x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_2 x^2 + b_1 x + b_0$ とすると、AND回路それぞれに特性多項式の係数 $b(b_{n-1}, \dots, b_1 = \text{係数 } s)$ が設定される。

[0022] 従って、 $b_j=0$ ($0 < j < n$) の時は、フリップフロップ FB_{j-1} ($0 < j < n$) から出力される値に関係なくAND回路からは“0”が出力され、 $b_j=1$ ($0 < j < n$) の時は、フリップフロップ FB_{j-1} ($0 < j < n$) から出力される値が出力される。

[0023] 次に、擬似乱数生成装置1Aの動作について、図4のフローチャートに基づいて説明する。

[0024] 擬似乱数生成装置1Aが擬似乱数生成の処理を開始すると、まず、初期値生成部4が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値 $ia(ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ と初期値 $ib(ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ を生成し(ステップS01)、それぞれの初期値を第1線形フィードバックシフトレジスタ2と第2線形フィードバックシフトレジスタ3へ供給する。

[0025] また、多項式係数生成部5が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第2線形フィードバックシフトレジスタ3の特性多項式の係数 $s(s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ を生成し(ステップS02)、第2線形フィードバックシフトレジスタ3へ供給する。

[0026] 第1線形フィードバックシフトレジスタ2と第2線形フィードバックシフトレジスタ3は、初期値生成部4と多項式係数生成部5から各初期値と係数が供給されると、各フリップフロップ回路とAND回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタ k の値を $k=0$ に設定する(ステップS03)。第1線形フィードバックシフトレジスタ2の各フリップフロップ回路 $FA_{m-1}, FA_{m-2}, \dots, FA_1, FA_0$ には、初期値 $ia(ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ が設定され、各AND回路には、原始多項式の係数 $a(a_{m-1}, \dots, a_1)$ が設定される。また、第2線形フィードバックシフトレジスタ3の各フリップフロップ回路 $FB_{n-1}, FB_{n-2}, \dots, FB_1, FB_0$ には、初期値 $ib(ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ が設定され、各AND回路

には、特性多項式の係数 $s(s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ が設定される。なお、図3の第2線形フィードバックシフトレジスタ3では、 $b_n=1$, $b_0=1$ としているが、 b_n および b_0 にAND回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

[0027] 次に、第1線形フィードバックシフトレジスタ2にクロック信号を入力すると(ステップS04)、第1線形フィードバックシフトレジスタ2は演算を行い、ビット ra_k を出力する(ステップS05)。同様に、第2線形フィードバックシフトレジスタ3にクロック信号を入力すると(ステップS06)、第2線形フィードバックシフトレジスタ3は演算を行い、ビット rb_k を出力する(ステップS07)。

[0028] 擬似乱数出力部6は、第1線形フィードバックシフトレジスタ2からビット ra_k が出力され、第2線形フィードバックシフトレジスタ3からビット rb_k が出力されると、両ビット値の排他的論理和を求めビット r_k を生成する(ステップS08)。

[0029] 次に、第1線形フィードバックシフトレジスタ2と第2線形フィードバックシフトレジスタ3は、カウンタ k の値を1つインクリメント($k \leftarrow k+1$)し(ステップS09)、カウンタ k の値が h の値を超えたかどうか判定する(ステップS10)。カウンタ k の値が h 以下の場合は、第1線形フィードバックシフトレジスタ2はステップS04に戻ってビット ra_{k+1} を出力し、第2線形フィードバックシフトレジスタ3はステップS06に戻ってビット rb_{k+1} を出力し、擬似乱数出力部6は、ビット r_{k+1} を生成する。

[0030] カウンタ k の値が h より大きい場合は、擬似乱数生成装置1は擬似乱数生成処理を終了し、これまでに生成されたビット $r_0, r_1, \dots, r_{h-1}, r_h$ が擬似乱数 $r(r_0, r_1, \dots, r_{h-1}, r_h)$ として出力される(ステップS11)。

[0031] ここで、図5を用いて具体的に説明する。一例として、8ビットの擬似乱数 r を出力するものとし、第1線形フィードバックシフトレジスタ2の原始多項式を x^7+x^3+1 とし、第1線形フィードバックシフトレジスタ2のフリップフロップ回路を7段構成として初期値 $ia(ia_6, ia_5, \dots, ia_1, ia_0)=(1, 0, 1, 0, 1, 0, 1)$ 、第2線形フィードバックシフトレジスタ3のフリップフロップ回路を8段構成として初期値 $ib(ib_7, ib_6, \dots, ib_1, ib_0)=(1, 1, 1, 1, 0, 0, 0, 0)$ 、第2線形フィードバックシフトレジスタ3の特性多項式の係数 $s(s_7, s_6, \dots, s_2, s_1)=(0, 1, 1, 1, 0, 1, 1)$ がそれぞれ設定されたとする。

[0032] まず、1回目のクロック信号が入力されると、第1線形フィードバックシフトレジスタ2

においては、 $FA_0 \rightarrow FA_1$ 、 $FA_1 \rightarrow FA_2$ 、 \dots 、 $FA_5 \rightarrow FA_6$ とビットがシフトして $(FA_6, FA_5, FA_4, FA_3, FA_2, FA_1) = (0, 1, 0, 1, 0, 1)$ となる。第1線形フィードバックシフトレジスタ2の原始多項式を $x^7 + x^3 + 1$ なので、 FA_6 のビット“1”は FA_2 から FA_3 へ出力されるビット“1”との排他的論理和“0”を FA_0 にフィードバックして図5の+1の状態になり、第1線形フィードバックシフトレジスタ2は“0”を ra_0 として出力する。

[0033] また、1回目のクロック信号が入力されると、第2線形フィードバックシフトレジスタ3においては、 $FB_0 \rightarrow FB_1$ 、 $FB_1 \rightarrow FB_2$ 、 \dots 、 $FB_6 \rightarrow FB_7$ とビットがシフトして $(FB_7, FB_6, FB_5, FB_4, FB_3, FB_2, FB_1) = (1, 1, 1, 0, 0, 0, 0)$ となる。特性多項式の係数 $s(s_7, s_6, \dots, s_2, s_1) = (0, 1, 1, 1, 0, 1, 1)$ から、特性多項式は $x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$ なので、 FB_5 から FB_6 へ出力されるビット“1”と、 FB_3 から FB_4 へ出力されるビット“0”と、 FB_1 から FB_2 へ出力されるビット“0”と、 FB_0 から FB_1 へ出力されるビット“0”との排他的論理和“1”を FB_0 にフィードバックして図5の+1の状態になり、第2線形フィードバックシフトレジスタ3は“1”を rb_0 として出力する。

[0034] 2回目のクロック信号が入力されると、第1線形フィードバックシフトレジスタ2および第2線形フィードバックシフトレジスタ3は、同様にビットシフトを行い、原始多項式と特性多項式に基づいてフィードバックを行い、図5の+2の状態となり、それぞれ $ra_1 = 0$ および $rb_1 = 1$ を出力する。

[0035] このように演算を繰り返すことによって、第1線形フィードバックシフトレジスタ2からは $(ra_0, ra_1, \dots, ra_6, ra_7) = (0, 0, 0, 0, 1, 0, 1, 1)$ 、第2線形フィードバックシフトレジスタ3からは $(rb_0, rb_1, \dots, rb_6, rb_7) = (1, 1, 1, 1, 1, 0, 0, 1)$ が出力され、 $(ra_0, ra_1, \dots, ra_6, ra_7) = (0, 0, 0, 0, 1, 0, 1, 1)$ と $(rb_0, rb_1, \dots, rb_6, rb_7) = (1, 1, 1, 1, 1, 0, 0, 1)$ との排他的論理和から擬似乱数 $r(r_0, r_1, \dots, r_6, r_7) = (1, 1, 1, 1, 0, 0, 1, 0)$ が出力される。

[0036] <第2の実施形態>

第2の実施形態における擬似乱数生成装置1Bは、図6に示すように、第1線形フィードバックシフトレジスタ2、第2線形フィードバックシフトレジスタ3、初期値生成部4、多項式係数生成部5、擬似乱数出力部6、原始多項式選択部7、および原始多項式記憶部8を有する。なお、第1の実施形態と同じものについては、同じ番号を付し、その詳細な説明を省略する。

- [0037] 原始多項式選択部7は、外部から入力される初期情報に従って、原始多項式記憶部8に記憶されている原始多項式を1つ選択し、特性多項式としてその原始多項式の係数 $a(a_{m-1}, \dots, a_1)$ を第1線形フィードバックシフトレジスタ2へ供給する機能を有する。
- [0038] 原始多項式記憶部8は、第1線形フィードバックシフトレジスタ2の各AND回路を設定するための原始多項式を識別情報と共に複数記憶する。なお、原始多項式を指定する識別情報としては番号を用いることができる。以下、識別番号と称する。この識別番号によって、原始多項式の係数より少ない情報量で各AND回路を設定することが可能であり、例えば、図6に示すように、ビット長を2ビットとすると、原始多項式記憶部8は、識別番号No.“00”は x^7+x^3+1 、識別番号No.“01”は $x^7+x^3+x^2+x+1$ 、識別番号No.“10”は $x^7+x^4+x^3+x^2+1$ 、識別番号No.“11”は $x^7+x^6+x^5+x^4+x^2+x+1$ というような原始多項式を記憶する。
- [0039] 次に、擬似乱数生成装置1Bの動作について、図7のフローチャートに基づいて説明する。
- [0040] 擬似乱数生成装置1Bが擬似乱数生成の処理を開始すると、まず、原始多項式選択部7が、外部から入力される初期情報に従って、原始多項式記憶部8から原始多項式を1つ選択し(ステップS21)、その選択した原始多項式の係数を特性多項式の係数 $a(a_{m-1}, \dots, a_1)$ として第1線形フィードバックシフトレジスタ2へ供給する。
- [0041] また、初期値生成部4は、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値 $ia(ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ と初期値 $ib(ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ を生成し(ステップS22)、それぞれの初期値を第1線形フィードバックシフトレジスタ2と第2線形フィードバックシフトレジスタ3へ供給する。
- [0042] また、多項式係数生成部5が、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第2線形フィードバックシフトレジスタ3の特性多項式の係数 $s(s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ を生成し(ステップS23)、第2線形フィードバックシフトレジスタ3へ供給する。
- [0043] 第1線形フィードバックシフトレジスタ2と第2線形フィードバックシフトレジスタ3は、原始多項式選択部7、初期値生成部4、および多項式係数生成部5から各初期値と

係数が供給されると、各フリップフロップ回路とAND回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタ k の値を $k=0$ に設定する(ステップS24)。第1線形フィードバックシフトレジスタ2の各フリップフロップ回路 $FA_{m-1}, FA_{m-2}, \dots, FA_1, FA_0$ には、初期値 $ia (ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ が設定され、各AND回路には、原始多項式選択部7から供給された特性多項式の係数 $a (a_{m-1}, \dots, a_1)$ が設定される。また、第2線形フィードバックシフトレジスタ3の各フリップフロップ回路 $FB_{n-1}, FB_{n-2}, \dots, FB_1, FB_0$ には、初期値 $ib (ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ が設定され、各AND回路には、特性多項式の係数 $s (s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ が設定される。なお、図3の第2線形フィードバックシフトレジスタ3では、 $b_n=1, b_0=1$ としているが、 b_n および b_0 にAND回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

[0044] 以降、第1の実施形態(ステップS04〜ステップS11)と同様の処理を行って擬似乱数 $r (r_0, r_1, \dots, r_{h-1}, r_h)$ を出力する(ステップS25〜ステップS32)。

[0045] <第3の実施形態>

第3の実施形態として、2つの擬似乱数生成装置1、例えば送信装置側に設けられた擬似乱数生成装置1と受信装置側に設けられた擬似乱数生成装置1とで特性多項式の係数と初期値(イニシャルデータ)を共有して、同じ擬似乱数を生成する擬似乱数生成装置1Cを示す。

[0046] 第3の実施形態における擬似乱数生成装置1Cは、図8に示すように、第1線形フィードバックシフトレジスタ2、第2線形フィードバックシフトレジスタ3、初期値生成部4、多項式係数生成部5、擬似乱数出力部6、原始多項式選択部7、原始多項式記憶部8、および通信部9を有する。なお、第1の実施形態および第2の実施形態と同じものについては、同じ番号を付し、その詳細な説明を省略する。また、便宜的に、イニシャルデータ送信側の擬似乱数生成装置1の構成要件には“t”の文字を、イニシャルデータ受信側の擬似乱数生成装置1の構成要件には“r”の文字を付す。

[0047] 通信部9は、原始多項式選択部7が選択した原始多項式の識別番号、初期値生成部4が生成した初期値 $ia (ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ および初期値 $ib (ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ 、多項式係数生成部5が生成した特性多項式の係数 $s (s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ を基に、原始多項式の識別番号、特性多項式の係数の初期値、および各初期値のそれ

ぞれのビット列からなるイニシャルデータを生成する機能、およびそのイニシャルデータを他の擬似乱数生成装置1と送受信する機能を有する。

[0048] また、通信部9は、イニシャルデータを受信した場合は、イニシャルデータから初期値 $ib(ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ と特性多項式の係数 $s(s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ とを抽出し、第2線形フィードバックシフトレジスタ3に供給する機能、イニシャルデータから初期値 $ia(ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ を抽出し、第1線形フィードバックシフトレジスタ2に供給する機能、イニシャルデータから原始多項式の識別番号を抽出し、原始多項式選択部7に供給する機能を有する。

[0049] 次に、2つの擬似乱数生成装置1Cで同じ擬似乱数を生成する際の動作について、図9のシーケンス図に基づいて説明する。

[0050] 擬似乱数生成装置1Ctが擬似乱数生成の処理を開始すると、まず、原始多項式選択部7tが、外部から入力される初期情報に従って、原始多項式記憶部8tから原始多項式を1つ選択し(ステップS41)、その選択した原始多項式の係数を特性多項式の係数 $a(a_{m-1}, \dots, a_1)$ として第1線形フィードバックシフトレジスタ2tへ供給すると共に、通信部9tへ原始多項式の識別番号を供給する。

[0051] また、初期値生成部4tは、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、初期値 $ia(ia_{m-1}, ia_{m-2}, \dots, ia_1, ia_0)$ と初期値 $ib(ib_{n-1}, ib_{n-2}, \dots, ib_1, ib_0)$ を生成し(ステップS42)、それぞれの初期値を第1線形フィードバックシフトレジスタ2t、第2線形フィードバックシフトレジスタ3t、および通信部9tへ供給する。

[0052] また、多項式係数生成部5tが、外部から入力される初期情報、あるいは予め定められた所定の条件に従って、第2線形フィードバックシフトレジスタ3tの特性多項式の係数 $s(s_{n-1}, s_{n-2}, \dots, s_2, s_1)$ を生成し(ステップS43)、第2線形フィードバックシフトレジスタ3tと通信部9tへ供給する。

[0053] 第1線形フィードバックシフトレジスタ2tと第2線形フィードバックシフトレジスタ3tは、原始多項式選択部7t、初期値生成部4t、および多項式係数生成部5tから各初期値と係数が供給されると、各フリップフロップ回路とAND回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタkの値を $k=0$ に設定する(ステップS44)。第1線形フィードバックシフトレジスタ2tの各フリップフロップ回路 $FA_{m-1}, FA_{m-2}, \dots,$

FA₁, FA₀ には、初期値ia (ia_{m-1}, ia_{m-2}, ..., ia₁, ia₀) が設定され、各AND回路には、原始多項式選択部7tから供給された特性多項式の係数a (a_{m-1}, ..., a₁) が設定される。また、第2線形フィードバックシフトレジスタ3tの各フリップフロップ回路FB_{n-1}, FB_{n-2}, ..., FB₁, FB₀ には、初期値ib (ib_{n-1}, ib_{n-2}, ..., ib₁, ib₀) が設定され、各AND回路には、特性多項式の係数s (s_{n-1}, s_{n-2}, ..., s₂, s₁) が設定される。なお、図3の第2線形フィードバックシフトレジスタ3tでは、b_n=1, b₀=1としているが、b_n およびb₀ にAND回路を設けて、他の係数と同様に任意の値を設定できるようにしてもよい。

[0054] また、通信部9tは、原始多項式の識別番号、特性多項式の係数、および各初期値のそれぞれのビット値からなるイニシャルデータを生成し擬似乱数生成装置1Crへ送信する(ステップS45)。この時、通信部9tは、所定の暗号化方式でイニシャルデータを暗号化して送信しても良い。

[0055] 例えば、原始多項式の識別番号が2ビット(“10”)、初期値iaが7ビット(“1010101”)、初期値ibが8ビット(“11110000”)、特性多項式の係数sが7ビット(“0111011”)であった場合、イニシャルデータは24ビットのデータ列(識別番号 | 初期値ia | 初期値ib | 係数s)=(101010101111100000111011)となる。

[0056] 以降、擬似乱数生成装置1Ctは、第1の実施形態(ステップS04〜ステップS11)と同様の処理を行って擬似乱数r (r₀, r₁, ..., r_{n-1}, r_n) を出力する(ステップS46〜ステップS51)。

[0057] 一方、擬似乱数生成装置1Crの通信部9rは、擬似乱数生成装置1Ctからイニシャルデータを受信すると(ステップS52)、イニシャルデータから初期値ib (ib_{n-1}, ib_{n-2}, ..., ib₁, ib₀) と特性多項式の係数s (s_{n-1}, s_{n-2}, ..., s₂, s₁) とを抽出し、第2線形フィードバックシフトレジスタ3rに供給し、イニシャルデータから初期値ia (ia_{m-1}, ia_{m-2}, ..., ia₁, ia₀) を抽出し、第1線形フィードバックシフトレジスタ2rに供給し、イニシャルデータから原始多項式の識別番号を抽出し、原始多項式選択部7rに供給する。なお、受信したイニシャルデータが暗号化されている場合は、通信部9rは、復号化してイニシャルデータを得る。

[0058] 原始多項式選択部7rは、原始多項式の識別番号が供給されると、その識別番号に該当する原始多項式を原始多項式記憶部8rから1つ選択し(ステップS53)、その選

択した原始多項式の係数を特性多項式の係数 $a(a_{m-1}, \dots, a_1)$ として第1線形フィードバックシフトレジスタ2rへ供給する。

[0059] また、第1線形フィードバックシフトレジスタ2rと第2線形フィードバックシフトレジスタ3rは、原始多項式選択部7r、および通信部9rから各初期値と各係数が供給されると、各フリップフロップ回路とAND回路に各初期値と係数を設定し、出力ビット数をカウントするカウンタkの値を $k=0$ に設定する(ステップS54)。

[0060] 以降、擬似乱数生成装置1Crは、第1の実施形態(ステップS04〜ステップS11)と同様の処理を行って擬似乱数 $r(r_0, r_1, \dots, r_{h-1}, r_h)$ を出力する(ステップS55〜ステップS60)。

[0061] このようにして、2つの擬似乱数生成装置1でイニシャルデータを共有することによって、同じ擬似乱数を生成することが可能となる。

[0062] なお、擬似乱数生成装置1は、上記の機能を記述した擬似乱数生成プログラムを汎用コンピュータに実行させることによって実現させても良い。この擬似乱数生成プログラムは、記録媒体から読み取られて汎用コンピュータに実行されても良いし、ネットワークを介して外部から伝送されて汎用コンピュータに実行されても良い。

産業上の利用可能性

[0063] 本発明によれば、常に所定のM系列より長い周期の擬似乱数列を生成することが可能となり、初期値だけでなく、特性多項式の係数も任意に設定できるため、生成された擬似乱数列を観測されてもその後生成される擬似乱数列を推測することは困難であり、生成される擬似乱数列の安全性を確保することができ、通信されるデータの安全性が保障される。識別情報と原始多項式との対応が分からなければ、通信されるデータの解読は困難である。

[0064] また、第1の線形フィードバックシフトレジスタの特性多項式として設定される原始多項式の選択には、その識別情報を用いることにより、係数を送受信するより少ないデータ量で済む。つまり、識別情報を原始多項式より少ない情報量とすれば、情報量を少なくすることができる。

請求の範囲

- [1] 所定のビット長の擬似乱数列を生成する擬似乱数生成装置(1)であって、
m段のシフトレジスタを有し、所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタ(2)と、
n段のシフトレジスタを有し、所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタ(3)と、
所定の条件に従って、前記第1の線形フィードバックシフトレジスタ(2)および前記第2の線形フィードバックシフトレジスタ(3)を構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタ(2)および前記第2の線形フィードバックシフトレジスタ(3)へ供給する初期値生成部(4)と、
所定の条件に従って、前記第2の線形フィードバックシフトレジスタ(3)の特性多項式の係数を生成し、前記第2の線形フィードバックシフトレジスタ(3)へ供給する多項式係数生成部(5)と、
前記第1の線形フィードバックシフトレジスタ(2)の特性多項式として原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶部(8)と、
所定の条件に従って、前記原始多項式記憶部(8)に記憶されている原始多項式を1つ選択し、その原始多項式の係数を特性多項式の係数として前記第1の線形フィードバックシフトレジスタ(2)へ供給する原始多項式選択部(7)と、
前記第1の線形フィードバックシフトレジスタ(2)から出力されるビット列と、前記第2の線形フィードバックシフトレジスタ(3)から出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力部(6)と、
を備えることを特徴とする擬似乱数生成装置(1)。
- [2] 前記擬似乱数生成装置(1C)は、
前記原始多項式選択部(7)によって選択された前記原始多項式の識別情報、前記初期値生成部(4)によって生成された前記第1の線形フィードバックシフトレジスタ(2)および前記第2の線形フィードバックシフトレジスタ(3)を構成する各シフトレジスタ

タの初期値、前記多項式係数生成部(5)によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成し、当該イニシャルデータを他の擬似乱数生成装置(1C)へ送出し、当該イニシャルデータを他の擬似乱数生成装置(1C)から受信した場合は、当該イニシャルデータから前記第1のフィードバックシフトレジスタ(2)と前記第2のフィードバックシフトレジスタ(3)との各初期値を抽出して前記第1の線形フィードバックシフトレジスタ(2)と前記第2の線形フィードバックシフトレジスタ(3)に供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第2の線形フィードバックシフトレジスタ(3)へ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択部(7)に供給する通信部(9)を備え、

前記原始多項式選択部(7)は、前記通信部(9)によって抽出された前記識別情報を基に、前記原始多項式記憶部(8)に記憶されている原始多項式を1つ選択し、その原始多項式の係数を前記第1の線形フィードバックシフトレジスタ(2)へ供給することを特徴とする請求の範囲第1項に記載の擬似乱数生成装置。

[3] 所定のビット長の擬似乱数列を生成するコンピュータによって実行される擬似乱数生成プログラムであって、

当該擬似乱数生成プログラムは、前記コンピュータを、

m段のシフトレジスタを有し、所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタと、

n段のシフトレジスタを有し、所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタと、

所定の条件に従って、前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタへ供給する初期値生成手段と、

所定の条件に従って、前記第2の線形フィードバックシフトレジスタの特性多項式の係数を生成し、前記第2の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、

前記第1の線形フィードバックシフトレジスタの特性多項式として原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶手段と、

所定の条件に従って、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を特性多項式の係数として前記第1の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、

前記第1の線形フィードバックシフトレジスタから出力されるビット列と、前記第2の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段と、

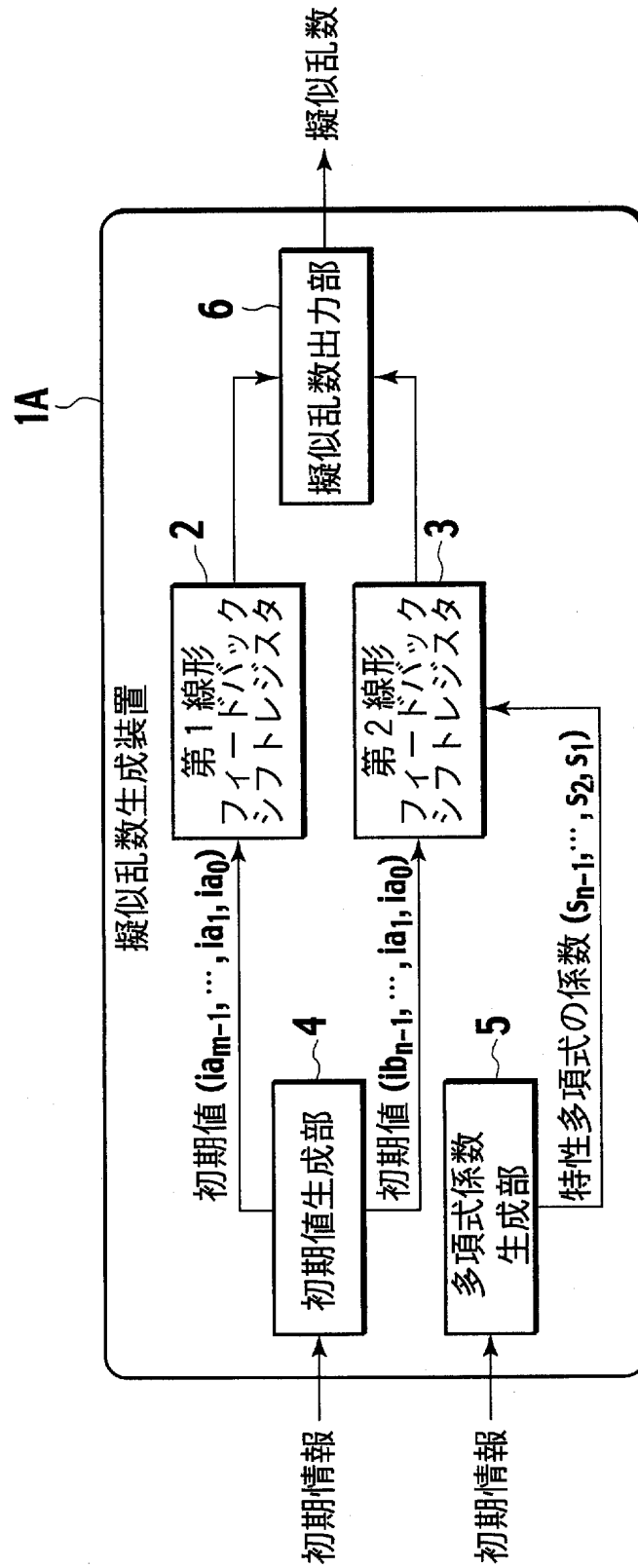
して機能させることを特徴とする擬似乱数生成プログラム。

[4] 前記擬似乱数生成プログラムは、前記コンピュータを、

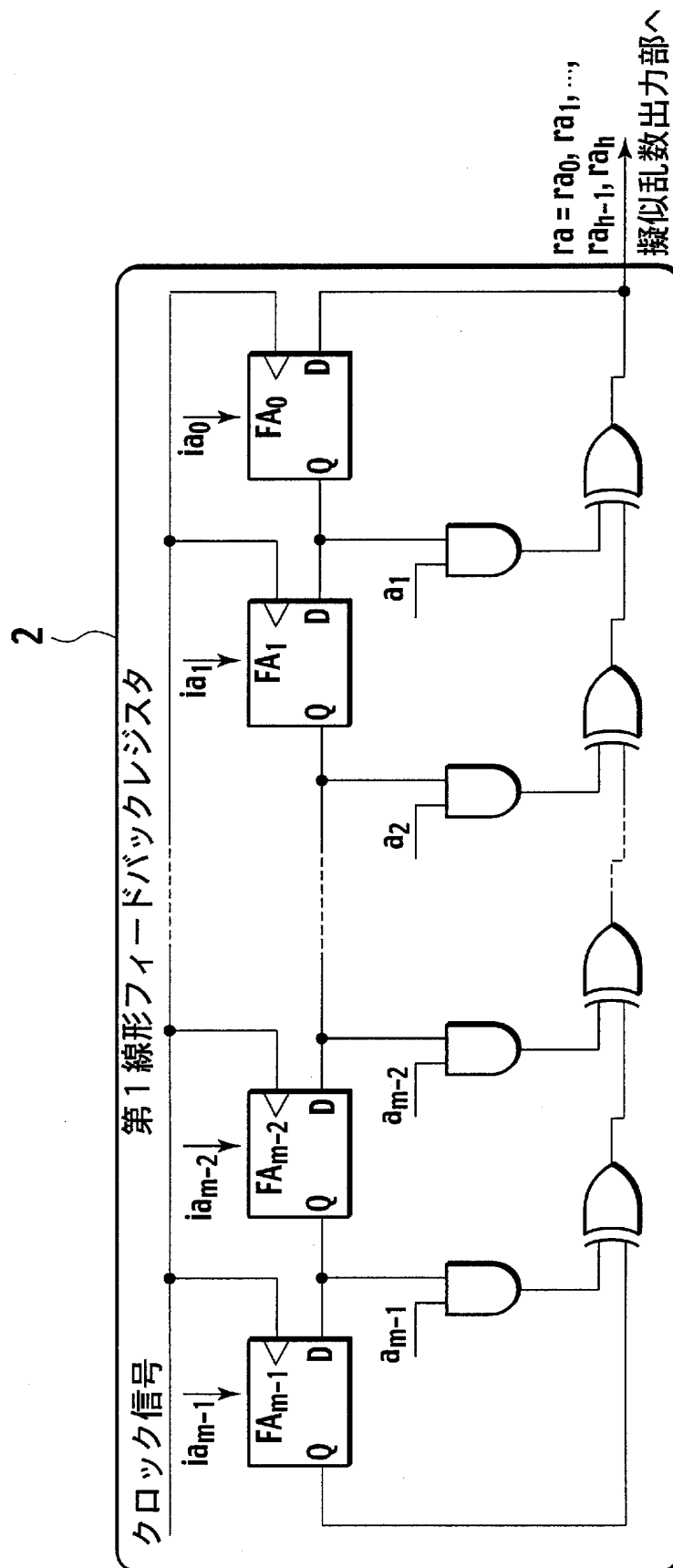
前記原始多項式選択手段によって選択された前記原始多項式の識別情報、前記初期値生成手段によって生成された前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタを構成する各シフトレジスタの初期値、前記多項式係数生成手段によって生成された前記特性多項式の係数のそれぞれからなるイニシャルデータを生成し、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第1のフィードバックシフトレジスタと前記第2のフィードバックシフトレジスタとの各初期値を抽出して前記第1の線形フィードバックシフトレジスタと前記第2の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記特性多項式の係数を抽出して前記第2の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、

前記原始多項式選択手段は、前記通信手段によって抽出された前記識別情報を基に、前記原始多項式記憶手段に記憶されている原始多項式を1つ選択し、その原始多項式の係数を前記第1の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする請求の範囲第3項に記載の擬似乱数生成プログラム。

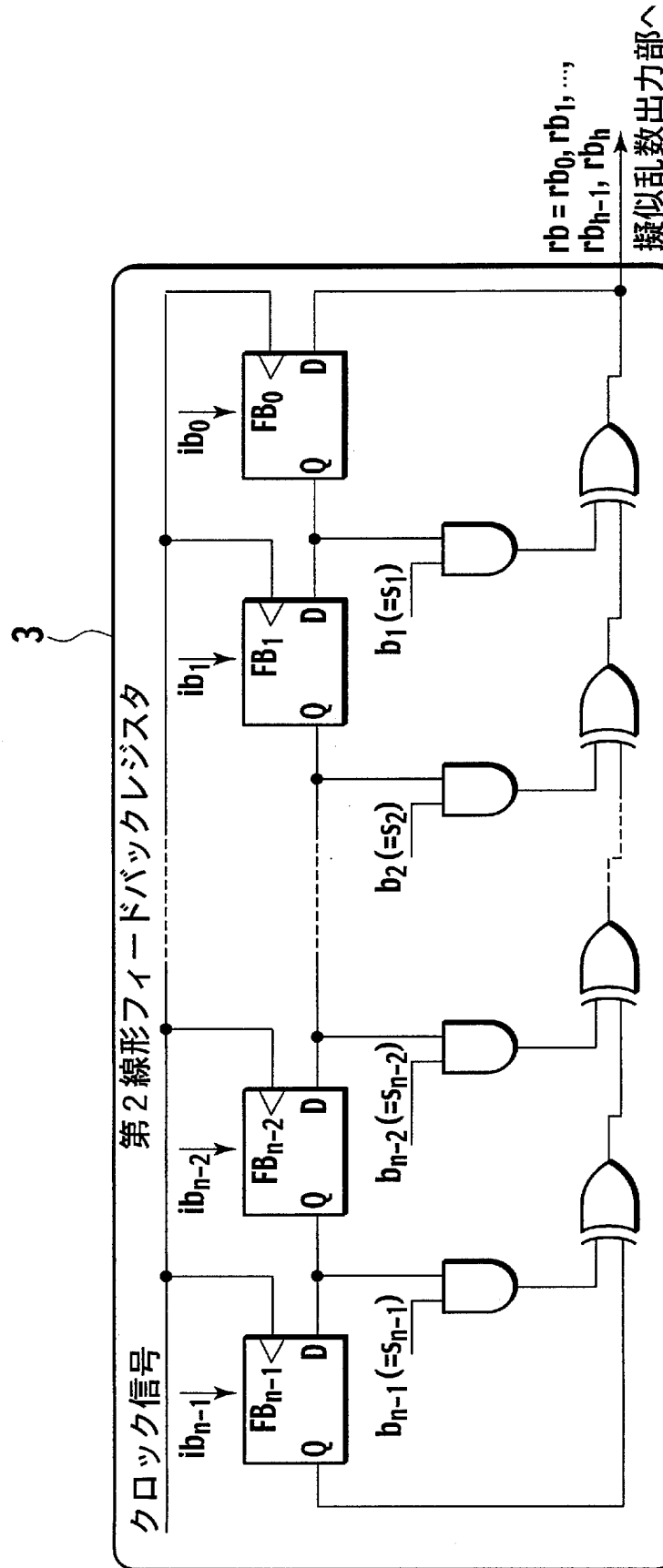
[図1]



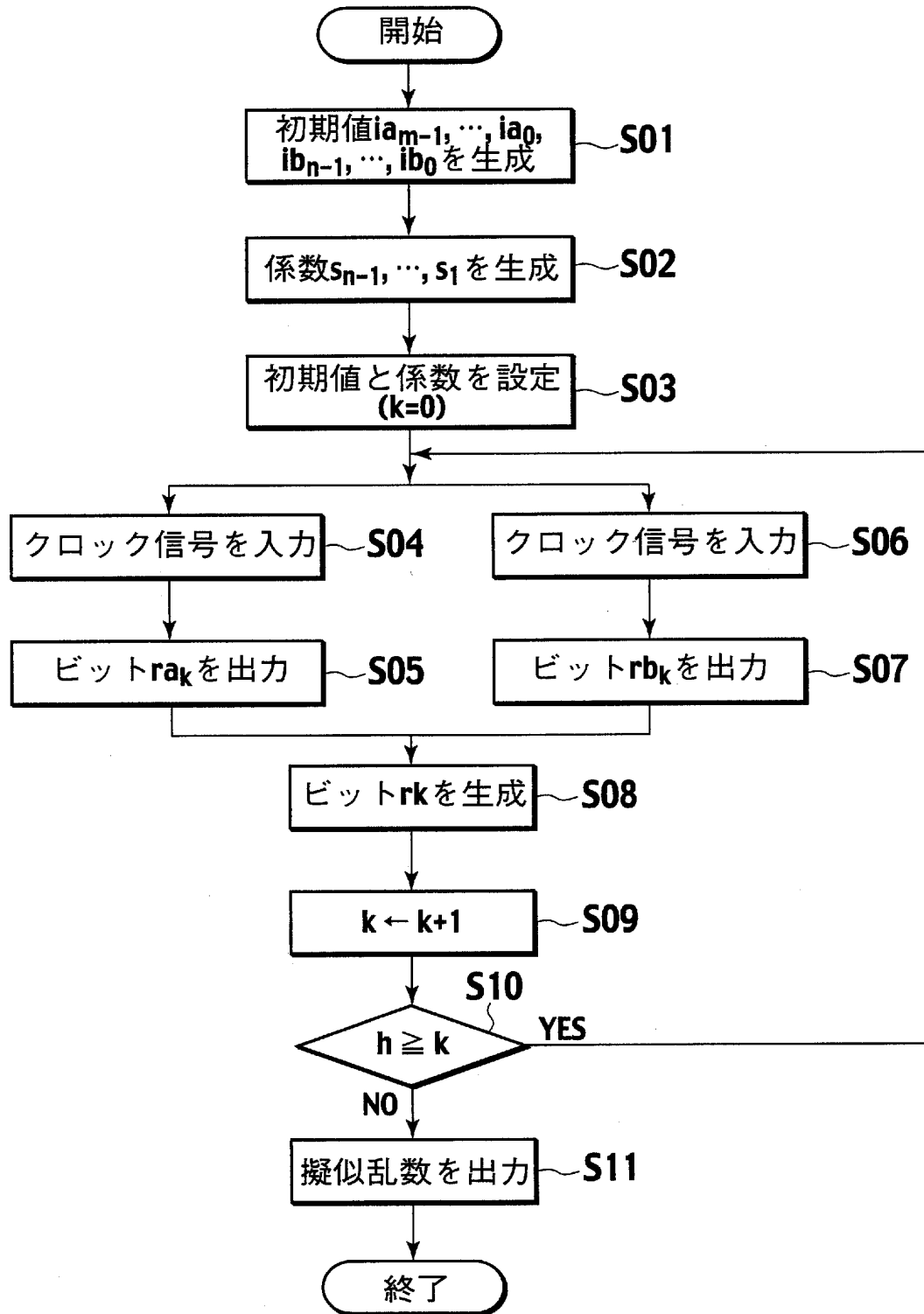
[図2]



[図3]



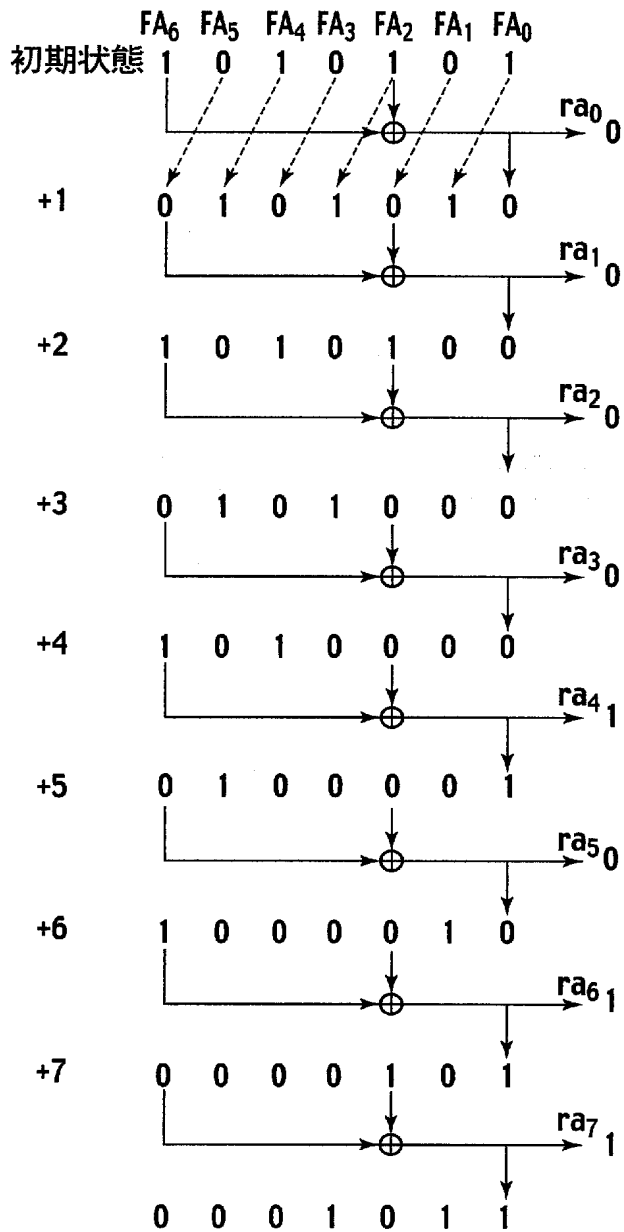
[図4]



[図5]

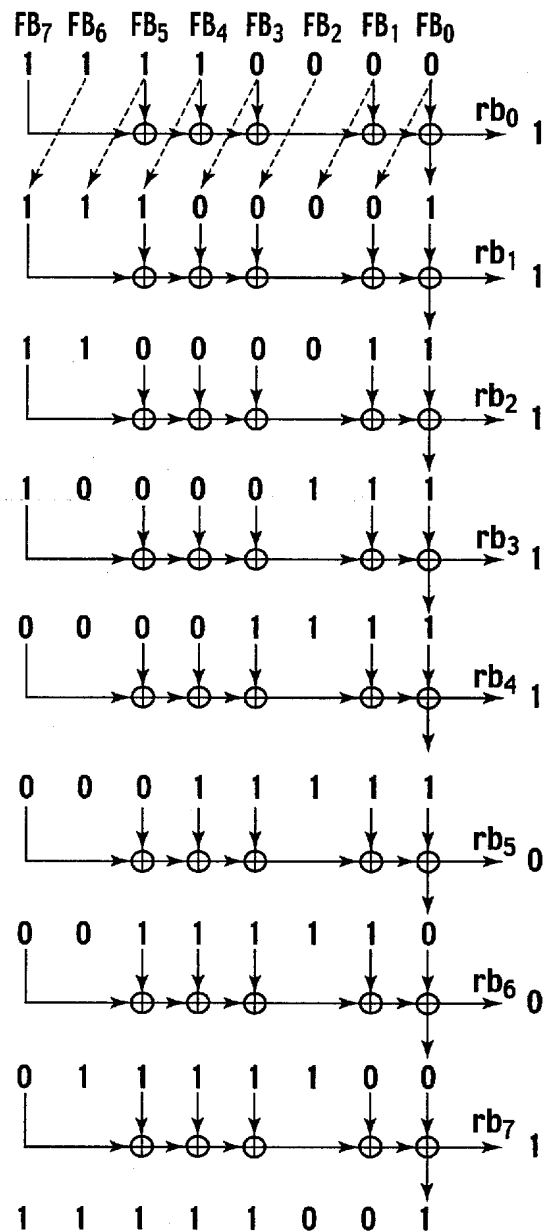
第1線形フィードバック シフトレジスタ

$$x^7 + x^3 + 1 \quad (a_6, a_5, a_4, a_3, a_2, a_1 = (000100))$$

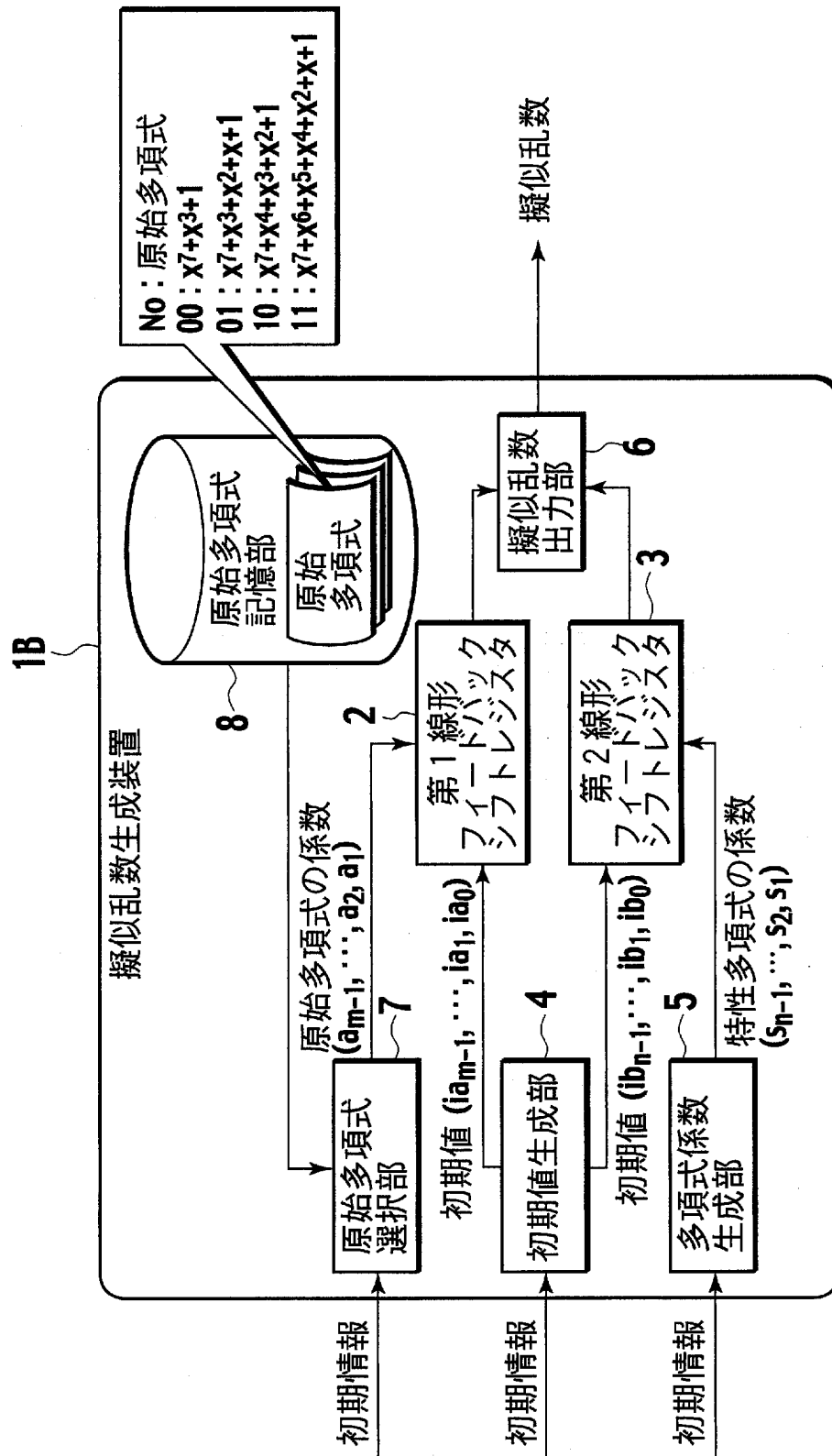


第2線形フィードバック シフトレジスタ

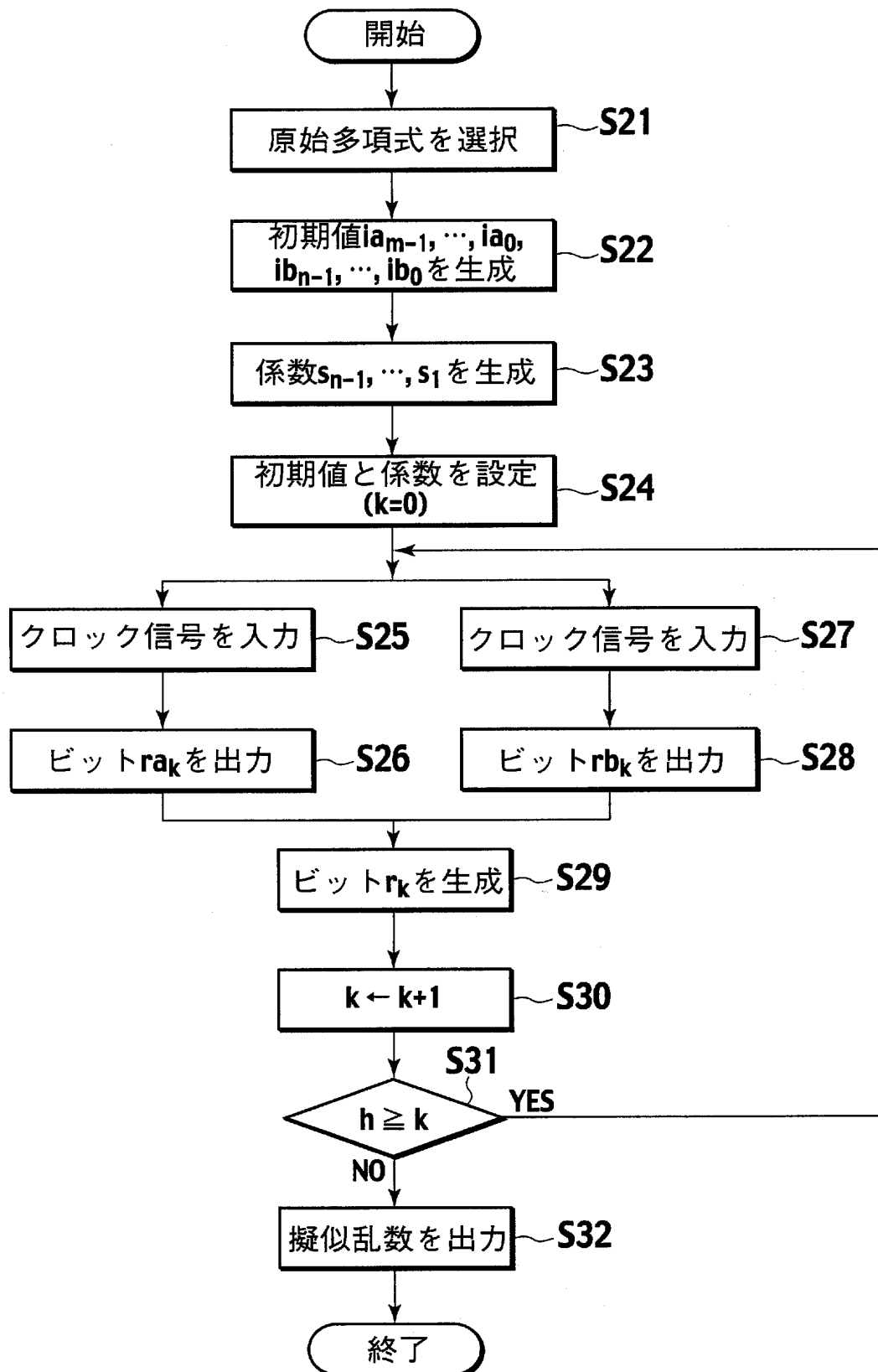
$$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$$



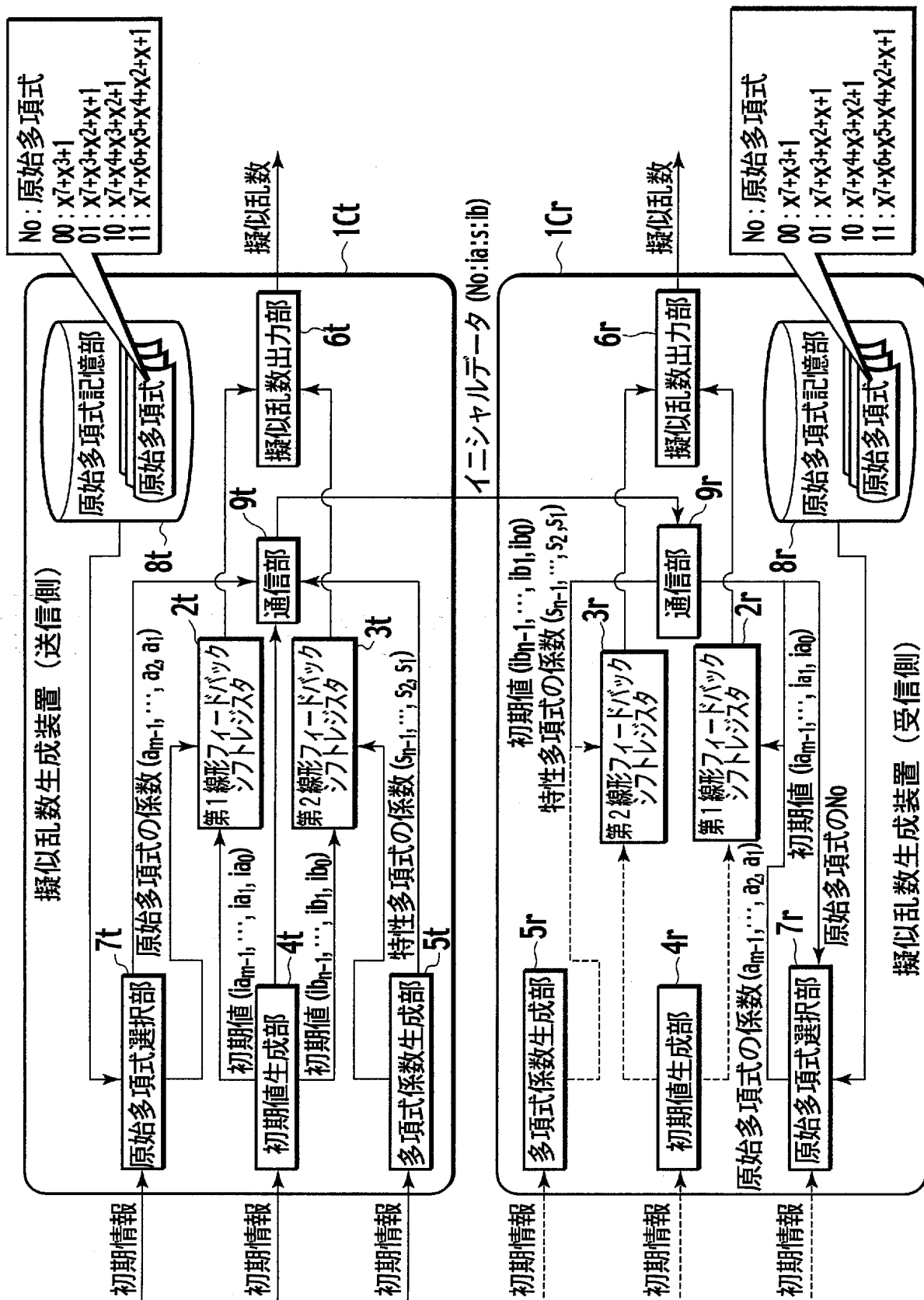
[図6]



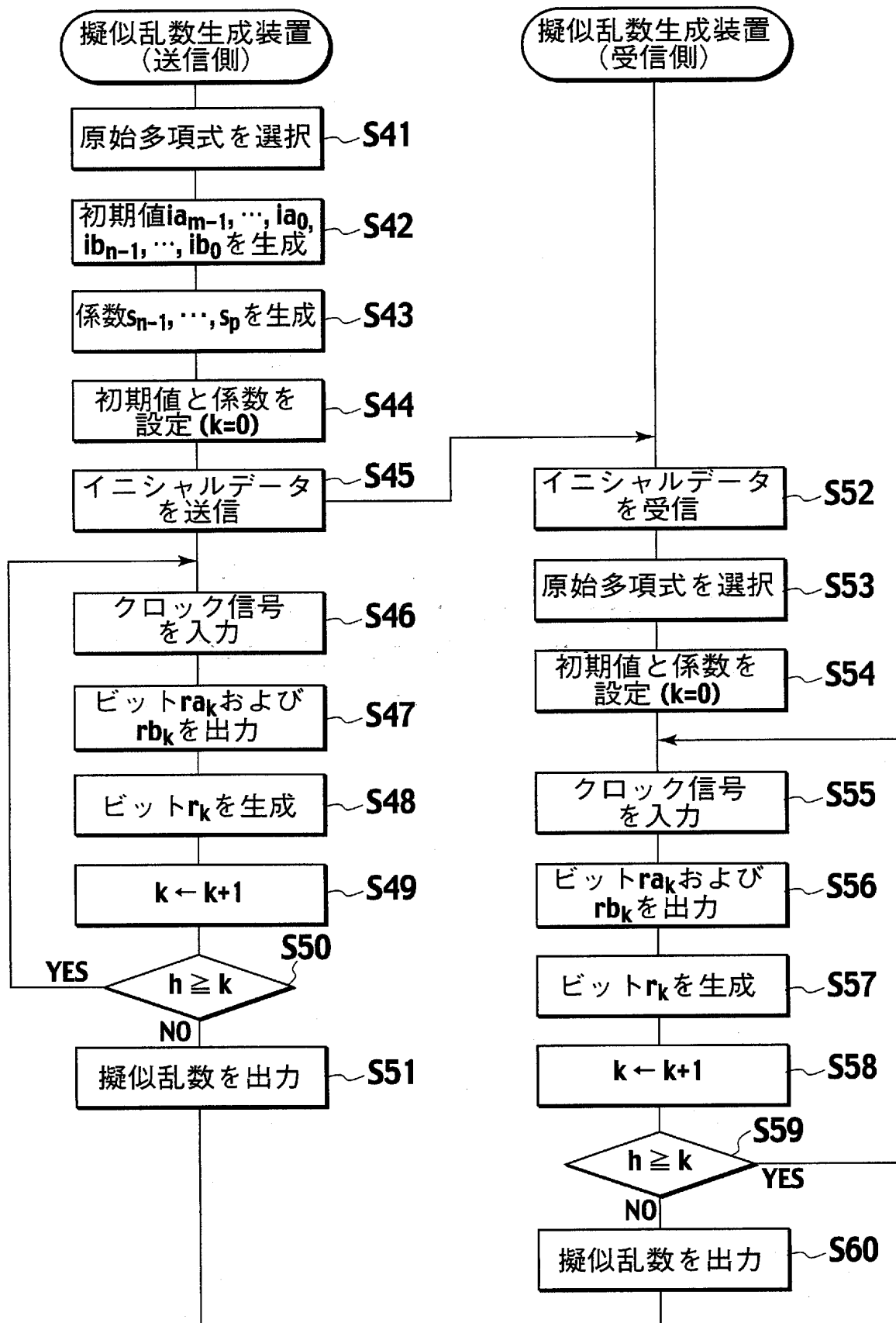
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/001211

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F7/58, H03K3/84

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F7/58, H03K3/84

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 9-179726 A (NEC Corp.), 11 July, 1997 (11.07.97), Full text; all drawings & EP 782069 A1	1-4
Y	JP 11-234096 A (Fujitsu Ltd.), 27 August, 1999 (27.08.99), Full text; all drawings & EP 938192 A2 & US 6275520 B1	1-4
Y	JP 61-141231 A (Sony Corp.), 28 June, 1986 (28.06.86), Full text; all drawings (Family: none)	1-4

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
26 April, 2005 (26.04.05)

Date of mailing of the international search report
17 May, 2005 (17.05.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl.⁷ G06F7/58, H03K3/84

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl.⁷ G06F7/58, H03K3/84

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 9-179726 A (日本電気株式会社) 1997.07.11, 全文、全図 & EP 782069 A1	1-4
Y	JP 11-234096 A (富士通株式会社) 1999.08.27, 全文、全図 & EP 938192 A2 & US 6275520 B1	1-4
Y	JP 61-141231 A (ソニー株式会社) 1986.06.28, 全文、全図 (ファミリー無し)	1-4

□ C欄の続きにも文献が列挙されている。

□ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリ

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

26.04.2005

国際調査報告の発送日

17.05.2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

山崎 慎一

5E

9174

電話番号 03-3581-1101 内線 3521